UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/738,807	12/13/2000	Jeremy Lawrence	81862.P178	2439

8791 7590 10/14/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
CHEN, ALAN S	
ART UNIT	**PAPER NUMBER**
2182	

DATE MAILED: 10/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/738,807	LAWRENCE, JEREMY	
	Examiner	Art Unit	
	Alan S. Chen	2182	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07/29/2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *47-69* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *47-69* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 April 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 07/29/2005 has been entered.

Response to Arguments

2. Applicant makes several arguments regarding the merit of using US Pat. No. 6,175,917 to Arrow et al. (Arrow) in the previous rejection. The Examiner does not agree with the arguments and his rebuttal is detailed below.

3. Applicant first argue data traveling over a public network is cannot be considered a "virtual private network" (VPN) since VPN connotes a private data network. Applicant appears to argue that since both data and management traffic goes over the public network, Fig. 1, element 100, such that the network is being shared by other computers then this cannot be considered a VPN. In other words, applicant is stating that the VPN requires essentially a dedicated line.

Examiner does not agree. First, it is well known to one of ordinary skill in the art that a VPN is a network that can use public networks as long as the path is secure and private in the sense that only the assigned source and destination. A widely accepted definition of VPN as per Netwon's Telecom Dictionary (attached) is as follows: "In contemporary usage, VPN most commonly refers to an IP VPN running over the public Internet. While the ubiquitous nature of the Internet is a huge advantage for data networking, the Internet is both insecure and subject to

variable levels of congestion. In order to create a VPN over the Internet, security issues are mitigated through the use of a combination of authentication, encryption and tunneling." Clearly, a VPN does not have to be a dedicated line; in fact that defeats the purpose of a VPN. A VPN is simply a *virtual* private line that can operate over a public network as long as only the permitted parties can see/hear the messages communicated in the communication path. To use the applicant's analogy, the truck using a road is like the packet for the traveling over the VPN. The road is indeed a VPN (more specifically a tunnel) if the goods within the truck are only known by the sender and the receiver and no one else. Secondly, Arrow clearly discloses that a VPN network that meets the definition of VPN as one of ordinary skill in the art would understand it. It is explicitly disclosed in Column 13, lines 3-15 that the VPN unit must authenticate the identity of the VPN management station 160 in order to ensure the security and integrity of the VPN unit. Furthermore, throughout Arrow, it is clear that a VPN is established between the VPN management station 160 and remote client 140. Column 6, lines 31-40 discloses the management station communicating with the VPN unit (elements 145, 115, 155, etc) over the public network which both being VPN units inherently would require the establishment of a secure line. Column 6, line 61-Column 7, line 5 disclose the VPN can only process packets that compressed, encrypted and authenticated. Column 8, lines 21+ and Fig. 3 disclose the flow chart of how the data packet is processed, e.g., requiring a secure line where the source and destination are members of the same VPN. And as mentioned before, the most specific disclosure of management data being sent over VPN is in Column 13, lines 3+ where configuration commands by the VPN management station 160 is received at the VPN and proper authentication and decryption are applied.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 47-69 are rejected under 35 U.S.C. 102(e) as being anticipated by Arrow.

6. Per claims 47, 52, 56, 61 and 66, Arrow discloses a method, network device and machine readable medium for secure in-band management of a network device (Fig. 2 and 3 show what happens at the VPN unit, utilizing compression, encryption and authentication rules to meets the definition of VPN, e.g., see Netwon's Telecom Dictionary; the network device is the entire unit, elements 140 and 145 of Fig. 1) that provides routing and forwarding services (both routing and forwarding services are provided by the VPN unit; Fig. 2, element 220-250 expressly show the VPN processing the message packet and forwarding the packet to the destination address; note that while there is a separate router for VPN to LAN connectivity, e.g., Fig. 1, element 110 to 114 to 115, it is clear that the same type of routing is performed at the remote clients, e.g., packetizing data to be sent over the public network, which the VPN unit is actually part of and hence the entire remote client is considered the "network device", e.g., 140 and 145 is a network device), the method comprising: configuring a VPN for the network device (VPN unit configures packets as for VPN by compression, encryption and authentication, element 240); linking the VPN to a source of management commands (Fig. 1, VPN management station 160 is linked to

VPN unit via VPN; Column 13, lines 3-15 and Fig. 7 show that the VPN unit is connected by VPN to the management station, where element 710, the configuration module resident on the VPN unit authenticates the configuration commands sent by the VPN management station); using the VPN to carry management traffic from the source of management commands to the network device (once authenticated, stream of data can pass through VPN from the management station 160 to the VPN unit, Column 13, lines 20-25); and using the network device (Fig. 7 is the OS of the VPN module which is part of the overall network device, elements 140 and 145, forwards management traffic to a management port (Fig. 7, elements 717 is the port where management data comes in and out of the VPN unit, which here is construed to be the VPN module; regarding what is forwarded out of the VPN unit, Arrow discloses various errors/confirmations that are reported back to the management station based on authentication results, Column 13, lines 15+). Note that the VPN used by Arrow by definition uses a tunneling protocol. Per Netwon's Telecom Dictionary, tunneling is defined as: "...the process of encapsulating an encrypted data packet in an IP packet for secure transmission across an inherently insecure IP network, such as the Internet". This is precisely what Arrow is performing, where the data is compressed, authenticated and encrypted and sent over the Internet (Fig. 2, elements 240 and 250). Further note the plurality of the network devices (Fig. 1 shows multiple remote client and VPN Units), all being capable of performing routing/forwarding and each having the management port of Fig. 7 to transfer router information (per claims 66).

7. Per claims 48,57 and 62, Arrow discloses the network device includes a routing and forwarding module (Fig. 7, elements 716 and 724 both route/forward the data packets) and the

management VPN module (VPN management station 160) that is coupled to the VPN unit via the public network (Fig. 1).

8. Per claims 49,53,58,63 and 67, Arrow discloses the network devices being a gateway (Fig. 1) per the definition of gateway from Netwon's telecom dictionary: "...an entrance and exit into a communications network". The gateway also meets the stricter definition of the word, which is a node between two networks, which is shown in Fig. 1, where the VPN unit and router, elements 114 and 116 sit between the public network and the LAN.

9. Per claims 50,54,59,64 and 68, Arrow discloses the network device can perform Internet Protocol services (Column 6, lines 50-55)

10. Per claims 51,55,60,65 and 69, Arrow discloses the source of management commands is one of a management device and management function (Fig. 1, element 160 is the management device, Column 13, lines 5+ disclose configuration request comments that is performed as a function of the management device).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The following patents are cited to further show the state of the art with respect to VPN networks and secure management commands:

U.S. Pat. No. US006832322B1 to Boden et al.

U.S. Pat. No. US006751729B1 to Giniger et al.

U.S. Pat. No. US006785728B1 to Schneider et al.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Alan S. Chen whose telephone number is 571-272-4143. The examiner can normally be reached on M-F 8:30am - 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on (571) 272-4083. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ASC
10/05/2005

KIM HUYNH
PRIMARY EXAMINER
10/11/05